UNITED STATES PATENT AND TRADEMARK OFFICE

nl

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/617,642	07/11/2003	Young Ho Park	46911/252170	5334

826 7590 05/01/2007

ALSTON & BIRD LLP
BANK OF AMERICA PLAZA
101 SOUTH TRYON STREET, SUITE 4000
CHARLOTTE, NC 28280-4000

EXAMINER	
DINH, MINH	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
05/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/617,642	PARK ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-10 and 12-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)□ Claim(s) _____ is/are rejected.

7)☒ Claim(s) *13,14,16,17,21,23,24,26-28 and 32* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 July 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 02/13/07. Claims 1, 7-9, 13-15, 17-18, 20, 22, 24-25, 28 and 31 have been amended; claims 5 and 11 have been cancelled. The specification has also been amended.

Response to Arguments

2. Applicant's arguments filed 2/13/07 have been fully considered but they are not persuasive. With respect to claim 1, Applicant argues that the XOR operation disclosed in Housley ("Alternate Temporal Key Hash") is not performed with respect to the first secret key and at least a portion of the MAC address (page 19, last paragraph). Housley discloses that TA, the MAC address of the transmitter, is assigned to part of array P1K (page 3, Section 3.1, PHASE1_STEP1; page 12), and this information is XORed with the first secret key TK (page 3, Section 3.1, PHASE1_STEP2). Applicant argues that Housley does not teach or suggest transforming the combination of the intermediate value with the predefined key change information by hashing (page 19, last paragraph). Housley discloses a hash function (i.e., Alternate Temporal Key Hash function) having two phases, wherein the result of phase 1 is combined with predefined key change information IV16 (page 4, Section 3.2, PHASE2_STEP1 and PHASE2_STEP2), and the combined data is further

transformed into a final key (page 4, Section 3.2, PHASE2_STEP2 and PHASE2_STEP3). Since the function is a hash function, the transforming of data utilizing by the hash function is part of hashing.

With respect to claim 12, Applicant argues that Housley does not disclose differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated (page 20, last paragraph). Housley discloses calculating a first secret key TK (Section 2, page 2) utilizing predefined key change information IV (i.e., using the IV value to determine when to calculate TK); determining if the IV has repeated (i.e., if the IV space is exhausted); differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated (i.e., stop using the current TK and wait for a new TK) than in instances in which the key change information has not repeated (i.e., using the current TK to generate an RC4 key for data encryption) (Section 5, page 5).

With respect to claims 15, 22 and 25, Applicant argues that none of the cited references teach or suggest: (i) determining if the predefined key change information has repeated; and (ii) generating the key for data encryption based upon the second temporary key and the determination if the predefined key change information has repeated (page 21, 2nd paragraph). Housley discloses determining whether the predefined key change information IV has repeated or not (i.e., whether the IV space is exhausted) and generating the key for data encryption based upon the second temporary key (Section 3.2, pages 3-4) as well as the result of the determining step (Section 5, page 5).

3. Applicant's arguments, see the 1st paragraph of page 20, filed 2/13/07, with respect to the rejection of claim 8 under 35 USC 102 have been fully considered and are persuasive. The rejection of claim 8 under 35 USC 102 has been withdrawn. However, the amendment has necessitated new grounds of rejection that are not based on prior art.

Claim Objections

4. Applicant is advised that should claim 1 be found allowable, claim 3 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 8-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 8 recites the limitation: permutating the intermediate value by (i) exchanging a selected number of bits of the IV value with an equal number of other bits of the IV value and (ii) outputting a result of a bitwise XOR operation and the exchange of the bits as a value that is bit shifted. However, both (i) and (ii) as claimed does not involve the intermediate value. It is unclear how to permutate a value without involving that value.

7. Claims 8-10 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. Claim 8 recites the limitation: "permutating the intermediate value by exchanging a selected number of bits of the IV value with an equal number of other bits of the IV value and outputting **a result of a bitwise XOR operation** and the exchange of the bits as a value that is bit shifted". The omitted elements

are: the inputs (i.e., operands) used in the bitwise XOR operation. Performing an XOR operation requires two inputs.

8. Claim 28 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 28, which depends on claim 25, recites the limitation "wherein the step of differently processing the secondary temporary key comprises ..." in line 2. There is insufficient antecedent basis for this limitation in the claim. For examination purposes, it is assumed that claim 28 depends on claim 26 (see claim 26, lines 2-3).

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

10. Claims 1-4, 6-7, 12, 15, 18-20, 22, 25 and 29-31 are rejected under 35 U.S.C. 102(a) as being anticipated by Housley et al. ("Alternate Temporal Key Hash"). Housley discloses a method and system for generating an RC4

key for use with WEP (Wired Equivalent Privacy) encryption algorithm in wireless LAN (Abstract; Section 1, Motivation).

Regarding claims 1-4 and 6, Housley specifically discloses a method for generating a key for data encryption comprising: selecting a first secret key (TK); combining the first secret key with at least a portion of a user-specific MAC address (TA) by performing a bitwise exclusive OR (XOR) operation to result in an intermediate value (P1K); combining the intermediate value with predefined key change information (IV16); and transforming the combination of the intermediate value and the predefined key change information by hashing to generate the key (RC4KEY) (Section 3, Alternate Temporal Key Hash Function, pages 3-4; page 12).

Regarding claim 7, Housley further discloses performing a bitwise XOR operation (Section 3.2, page 4).

Regarding claim 12, Housley discloses a method for generating a key for data encryption comprising: calculating a first secret key utilizing predefined key change information (Section 3, Alternate Temporal Key Hash Function); determining if the key change information has repeated or not (Section 5, Initialization Vector Management); and differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated (Section 5, Initialization Vector Management).

Regarding claims 15, 18-20, 22, 25, 27 and 29-31, Housley discloses a method for generating a key for data encryption comprising: selecting a first secret key (TK); generating a first temporary key (P1K) based upon a combination of the first secret key with a MAC address (TA) and further based upon predefined key change information (IV counter) and hashing; generating a second temporary key (RC4KEY) based upon a combination of the first temporary key and an IV value (IV counter) (Section 3, Alternate Temporal Key Hash Function); determine if the predefined key change information has repeated; setting the second temporary key to be the final key for data encryption if the predefined key change information has not repeated; encrypting data to be transmitted with the final key (Section 5, Initialization Vector Management).

Allowable Subject Matter

11. Claims 8-10 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

12. Claims 13-14, 16-17, 21, 23-24, 26-28 and 32 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Housley et al., "Temporal Key Hash"

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD
Minh Dinh
Examiner
Art Unit 2132

4/27/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100